A characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field[☆]

Gerardo Vega

Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 México D.F., Mexico, gerardov@unam.mx

Abstract

It is well known that the problem of determining the weight distributions of families of cyclic codes is, in general, notoriously difficult. An even harder problem is to find characterizations of families of cyclic codes in terms of their weight distributions. On the other hand, it is also well known that cyclic codes with few weights have a great practical importance in coding theory and cryptography. In particular, cyclic codes having three nonzero weights have been studied by several authors, however, most of these efforts focused on cyclic codes over a prime field. In this work we present a characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field. The codes under this characterization are, indeed, optimal in the sense that their lengths reach the Griesmer lower bound for linear codes. Consequently, these codes reach, simultaneously, the best possible coding capacity, and also the best possible capabilities of error detection and correction for linear codes. But because they are cyclic in nature, they also possess a rich algebraic structure that can be utilized in a variety of ways, particularly, in the design of very efficient coding and decoding algorithms. What is also worth pointing out, is the simplicity of the necessary and sufficient numerical conditions that characterize our class of optimal three-weight cyclic codes. As we already pointed out, it is a hard problem to find this kind of characterizations. However, for this particular case the fundamental tool that allowed us to find our characterization was the characterization for all two-weight irreducible cyclic codes that was introduced by B. Schmidt and C. White

[☆] Partially supported by PAPIIT-UNAM IN107515.

(2002). Lastly, another feature about the codes in this class, is that their duals seem to have always the same parameters as the best known linear codes.

Keywords: Cyclic codes, weight distribution, Gaussian sums, Griesmer lower bound
2000 MSC: 11T71, 11T55, 12E20

1. Introduction

The weight distribution of a code is important because it plays a significant role in determining their capabilities of error detection and correction. For cyclic codes this problem gains greater interest due mainly to the fact that they possess a rich algebraic structure. However, as was pointed out by C. Ding (2009), the problem of determining the weight distributions of families of cyclic codes is, in general, notoriously difficult. An even harder problem is to find characterizations for these families of cyclic codes in terms of their weight distributions. In fact, very few characterizations of this kind are known. One of the first and most relevant efforts in that direction is the work of B. Schmidt and C. White (2002), where simple necessary and sufficient numerical conditions for an irreducible cyclic code to have at most two weights, are presented. Along the same lines, there also exists a set of characterizations, for the one-weight irreducible cyclic codes that was introduced in G. Vega (2007). In the case of reducible cyclic codes a characterization for the two-weight projective cyclic codes, was recently presented by T. Feng (2015).

On the other hand, it is also well known that cyclic codes with few weights have a great practical importance in coding theory and cryptography, and this is so because they are useful in the design of frequency hopping sequences and in the development of secret sharing schemes. Some work has already been done in relation with irreducible and reducible two-weight cyclic codes (see for example, B. Schmidt and C. White (2002), G. Vega (2008) and T. Feng (2015)), however we believe that for the particular case of reducible three-weight cyclic codes, whose duals have two zeros, a more in-depth study is possible. For example, cyclic codes having three weights have been studied by several authors (see for example, J. Yuan, C. Carlet *et al.* (2006), Z. Zhou and C. Ding (2013) and C. Li, N. Li, *et al.* (2014)), however most of the efforts in that direction have been focused on cyclic codes over a prime field. In this work we present a characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field. The codes in this class are, indeed, optimal in the sense that their lengths reach the Griesmer lower bound for linear codes. Therefore, in addition to the rich algebraic structure that is intrinsically associated with all cyclic codes, our codes also reach the best possible coding capacity, and also they have the best possible capabilities for error detection and correction for linear codes. As a further result of this work, we also find the parameters for the dual code of any cyclic code in our characterized class. In fact, throughout several studied examples, it seems that such dual codes always have the same parameters as the best known linear codes.

TABLE I

Weight distribution of $\mathcal{C}_{((q+1)e_1,e_2)}$.

Weight	**Frequency**
0	1
$q(q-1)-1$	$(q-1)(q^2-1)$
$q(q-1)$	q^2-1
q^2-1	$q-1$

In order to provide a detailed explanation of what is the main result of this work, let q be the power of a prime number, and also let γ be a fixed primitive element of $\mathbb{F}_{q^2}$. For any integer a, denote by $h_a(x) \in \mathbb{F}_q[x]$ the minimal polynomial of γ^{-a}. With this notation in mind, the following result gives a full description for the weight distribution of a class of optimal three-weight cyclic codes of length q^2-1, dimension 3 over the finite field $\mathbb{F}_q$.

Theorem 1. *For any two integers e_1 and e_2, let $\mathcal{C}_{((q+1)e_1,e_2)}$ be the cyclic code, over $\mathbb{F}_q$, whose parity-check polynomial is $h_{(q+1)e_1}(x)h_{e_2}(x)$. Thus, if* $\gcd(q-1, 2e_1-e_2)=1$ *and* $\gcd(q+1, e_2)=1$ *then*

(A) $\deg(h_{(q+1)e_1}(x)) = 1$ *and* $\deg(h_{e_2}(x)) = 2$. *In addition, $h_{(q+1)e_1}(x)$ and $h_{e_2}(x)$ are the parity-check polynomials of two different one-weight cyclic codes of length q^2-1, whose nonzero weights are, respectively, q^2-1 and $q(q-1)$.*

(B) $\mathcal{C}_{((q+1)e_1,e_2)}$ *is an optimal three-weight* $[q^2-1, 3, q(q-1)-1]$ *cyclic code over* $\mathbb{F}_q$*, with the weight distribution given in Table I. In addition, if* B_j*, with* $0 < j \leq q^2-1$*, is the number of words of weight* j *in the dual code of* $\mathcal{C}_{((q+1)e_1,e_2)}$*, then* $B_1 = B_2 = 0$ *and*

$$B_3 = \frac{(q^2-3)(q^2-1)(q-2)(q-1)}{6} \ .$$

Therefore, if $q > 2$*, then the dual code of* $\mathcal{C}_{((q+1)e_1,e_2)}$ *is a single-error-correcting cyclic code with parameters* $[q^2-1, q^2-1-3, 3]$.

For the particular case when q is an even integer, and in connection with the class cyclic codes given by Theorem 1, the following result was recently presented in C. Li, Q. Yue, *et al.* (2014).

Theorem 2. *With our notation, suppose that* q *is an even integer. Then* $\mathcal{C}_{(q+1,q-1)}$ *is a three-weight* $[q^2-1, 3, q(q-1)-1]$ *cyclic code over* $\mathbb{F}_q$*, with the weight distribution given in Table I.*

Now, since q is an even integer, clearly $\gcd(q-1, 2(1)-(q-1)) = \gcd(q-1, 2) = 1$ and $\gcd(q+1, q-1) = 1$. Therefore, it is interesting to observe that the family of codes given by the previous theorem are completely contained in the class of cyclic codes studied by Theorem 1. Therefore our main result not only extends the family of codes in Theorem 2, but also it extends the previous result to cyclic codes over *any* finite field. In fact, this is not all that can be said because, as will be outlined below, all cyclic codes, over $\mathbb{F}_q$, of length q^2-1, whose weight distributions are given in Table I, satisfy the two easy-to-check conditions in Theorem 1. In other words, Theorem 1 is, indeed, a characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field. As we already pointed out, it is a hard problem to find this kind of characterizations. However, for this particular case the fundamental tool that allowed us to find our characterization was, as will be shown later, the characterization for all two-weight irreducible cyclic codes that was introduced by B. Schmidt and C. White (2002).

This work is organized as follows: In Section 2 we establish our notation and recall the definition for the Gaussian sums. Section 3 is devoted to recalling the Griesmer lower bound, and also to presenting a result that will allow us to conclude that the class of codes in Theorem 1 are optimal in the sense that their lengths reach such lower bound. In Section 4 we will study a kind of exponential sums that is important in order to determine the weights, and their corresponding frequencies, of the codes in Theorem 1. In fact, for this kind of exponential sums, we are going to find simple necessary and sufficient numerical conditions in order that the evaluation of any exponential sum of such kind is exactly equal to one. In Section 5 we use the definitions and results of the previous sections in order to present a formal proof of Theorem 1. After this, we will analyze the two easy-to-check conditions of Theorem 1 in order to give an explicit formula for the number of cyclic codes that satisfy such conditions. In addition we include, at the end of this section, some examples of Theorem 1 as well as some examples of such explicit formula. In Section 6 we will prove that the two easy-to-check sufficient numerical conditions in Theorem 1 are also the necessary conditions. Finally Section 7 will be devoted to present ours conclusions.

2. Notation and some definitions

First of all we set for this section and for the rest of this work, the following:

Notation. By using q we will denote the power of a prime number, whereas by using γ we will denote a fixed primitive element of $\mathbb{F}_{q^2}$. We are going to fix $\delta := \gamma^{q+1}$, and consequently note that δ is a fixed primitive element of $\mathbb{F}_q$. For any integer a, the polynomial $h_a(x) \in \mathbb{F}_q[x]$ will denote the minimal polynomial of γ^{-a}. In addition, we will denote by "$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$" the trace mapping from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$.

An important tool for this work are the so-called Gaussian sums. Thus, in order to recall such tool, let ψ be a multiplicative and χ an additive character of a finite field F. Then the *Gaussian sum*, $G_F(\psi, \chi)$, of the characters ψ and χ over F is defined by

$$G_F(\psi, \chi) := \sum_{c \in F^*} \psi(c)\chi(c) \ .$$

There are several other results related to Gaussian sums that will be important for this work. Fortunately, these results are perfectly well explained in Chapter 5 of R. Lidl and H. Niederreiter (1984).

3. The Griesmer lower bound

Let $n_q(k,d)$ be the minimum length n for which an $[n,k,d]$ linear code, over $\mathbb{F}_q$, exists. Given the values of q, k and d, a central problem of coding theory is to determine the actual value of $n_q(k,d)$. A well-known lower bound (see J.H. Griesmer (1960) and G. Solomon and J.J. Stiffler (1965)) for $n_q(k,d)$ is

Theorem 3. *(Griesmer bound) With the previous notation,*

$$n_q(k,d) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \ .$$

With the aid of the previous lower bound, we now present the following result.

Lemma 1. *Suppose that $\mathcal{C}$ is a $[q^2-1, 3, q(q-1)-1]$ linear code over $\mathbb{F}_q$. Then $\mathcal{C}$ is an optimal linear code in the sense that its length reaches the lower bound in previous theorem.*

Proof: By means of a direct application of the Griesmer lower bound, we have

$$\begin{aligned} & \left\lceil \frac{q(q-1)-1}{q^0} \right\rceil + \left\lceil \frac{q(q-1)-1}{q} \right\rceil + \left\lceil \frac{q(q-1)-1}{q^2} \right\rceil \\ = \ & [(q-1)q-1] + [q-1] + 1 = q^2 - 1 \ . \end{aligned}$$

□

4. A class of exponential sums

It is well known that the weight distribution of some cyclic codes can be obtained by means of the evaluation of some exponential sums. This is particularly true for the class of cyclic codes that we are interested in. The following result goes along these lines.

Lemma 2. *Let χ' and χ be respectively the canonical additive characters of $\mathbb{F}_{q^2}$ and $\mathbb{F}_q$. For any integers e_1 and e_2, and for all $a, b \in \mathbb{F}_{q^2}$, consider the sums*

$$S_{(e_1,e_2)}(a,b) := \sum_{x \in \mathbb{F}_{q^2}^*} \chi'(ax^{(q+1)e_1} + bx^{e_2}) \; .$$

If $a^q + a \neq 0$, $b \neq 0$ and $\gcd(q+1, e_2) = 1$, then

$$S_{(e_1,e_2)}(a,b) = -\sum_{z \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q^*} \chi(z + (a^q + a)x^{e_1} + z^{-1}b^{q+1}x^{e_2}) \; .$$

Proof: Recalling that $\delta := \gamma^{q+1}$ we have

$$\begin{aligned} S_{(e_1,e_2)}(a,b) &= \sum_{i=0}^{q-2} \chi'(a\delta^{ie_1}) \sum_{w \in \gamma^i \langle \gamma^{q-1} \rangle} \chi'(bw^{e_2}) \\ &= \sum_{i=0}^{q-2} \chi(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a)\delta^{ie_1}) \sum_{w \in \gamma^i \langle \gamma^{q-1} \rangle} \chi'(bw^{e_2}) \; , \end{aligned}$$

and, since $\gcd(q+1, e_2) = 1$, we have

$$\sum_{w \in \gamma^i \langle \gamma^{q-1} \rangle} \chi'(bw^{e_2}) = \sum_{w \in \gamma^{ie_2} \langle \gamma^{q-1} \rangle} \chi'(bw) = \frac{1}{q-1} \sum_{w \in \mathbb{F}_{q^2}^*} \chi'(b\gamma^{ie_2} w^{q-1}) \; .$$

Let $\widehat{\mathbb{F}}_{q^2}$ and $\widehat{\mathbb{F}}_q$ be respectively the multiplicative character groups of $\mathbb{F}_{q^2}$ and $\mathbb{F}_q$. Now, if N is the norm mapping from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ and H is the subgroup of order $q-1$ of $\widehat{\mathbb{F}}_{q^2}$, then note that $H = \{\psi \circ \mathrm{N} \mid \psi \in \widehat{\mathbb{F}}_q\}$ (that is, H is nothing but the "lift" of $\widehat{\mathbb{F}}_q$ to $\mathbb{F}_{q^2}$). Therefore, owing to Theorem 5.30 (p. 217) in R. Lidl and H. Niederreiter (1984), we have

$$\begin{aligned} \sum_{w \in \mathbb{F}_{q^2}^*} \chi'(b\gamma^{ie_2} w^{q-1}) &= \sum_{\psi \in \widehat{\mathbb{F}}_q} G_{\mathbb{F}_{q^2}}(\bar{\psi} \circ \mathrm{N}, \chi') \psi(\mathrm{N}(b\gamma^{ie_2})) \\ &= -\sum_{\psi \in \widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\bar{\psi}, \chi)^2 \psi(\mathrm{N}(b\gamma^{ie_2})) \; , \end{aligned}$$

where the last equality arises due to the Davenport-Hasse theorem (Theorem 5.14 (p. 197) in R. Lidl and H. Niederreiter (1984)). In consequence, since $\gamma^{i(q+1)} = \mathrm{N}(\gamma^i) = \mathrm{N}(\gamma)^i = \delta^i$ and $\langle\delta\rangle = \mathbb{F}_q^*$, we have

$$S_{(e_1,e_2)}(a,b) = -\frac{1}{q-1} \sum_{x\in\mathbb{F}_q^*} \chi((a^q+a)x^{e_1}) \sum_{\psi\in\widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\bar{\psi},\chi)^2 \psi(b^{q+1}x^{e_2}) \ . \quad (1)$$

On the other hand, by using the Fourier expansion of the restriction of χ to $\mathbb{F}_q^*$ in terms of the multiplicative characters of $\mathbb{F}_q$, we have that for all $x, z \in \mathbb{F}_q^*$:

$$\chi(z^{-1}b^{q+1}x^{e_2}) = \frac{1}{q-1} \sum_{\psi\in\widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\bar{\psi},\chi)\bar{\psi}(z)\psi(b^{q+1}x^{e_2}) \ ,$$

and by multiplying both sides of the preceding equation by $\chi(z)$ and by summing we obtain

$$\sum_{z\in\mathbb{F}_q^*} \chi(z + z^{-1}b^{q+1}x^{e_2}) = \frac{1}{q-1} \sum_{\psi\in\widehat{\mathbb{F}}_q} G_{\mathbb{F}_q}(\bar{\psi},\chi)^2 \psi(b^{q+1}x^{e_2}) \ .$$

Finally, by substituting the previous equation in (1) we obtain the desired result. □

Remark 1. *It is worth pointing out that an important part of the previous proof was inspired by the proof of Theorem 2.8 in M.J. Moisio (1997).*

Now we are going to analyze a kind of exponential sums that are constructed by means of those exponential sums studied in the previous lemma. In fact, in what follows we are going to find simple necessary and sufficient numerical conditions in order that the evaluation of any exponential sum of such kind is exactly equal to one.

Lemma 3. *With the same notation and hypothesis as in the previous lemma, consider now the sums of the form:*

$$T_{(e_1,e_2)}(a,b) := \sum_{y\in\mathbb{F}_q^*} S_{(e_1,e_2)}(ya,yb) \ .$$

Then $\gcd(q-1, 2e_1-e_2) = 1$ *if and only if* $T_{(e_1,e_2)}(a,b) = 1$.

Proof: Suppose that $\gcd(q-1, 2e_1 - e_2) = 1$, then, from previous lemma and since $y^{q+1} = y^2$ for all $y \in \mathbb{F}_q^*$, we have

$$T_{(e_1,e_2)}(a,b) = -\sum_{y\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_q^*}\chi(z + (a^q+a)x^{e_1}y + z^{-1}b^{q+1}x^{e_2}y^2)\ . \qquad (2)$$

First suppose that q is even. Then by Theorem 5.34 (p. 218) in R. Lidl and H. Niederreiter (1984) we know that, for all $\rho_0, \rho_1, \rho_2 \in \mathbb{F}_q$,

$$\sum_{y\in\mathbb{F}_q}\chi(\rho_0 + \rho_1 y + \rho_2 y^2) = \begin{cases} \chi(\rho_0)q & \text{if } \rho_2 + \rho_1^2 = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned} T_{(e_1,e_2)}(a,b) &= 1 - q - \sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q}\chi(z + (a^q+a)x^{e_1}y + z^{-1}b^{q+1}x^{e_2}y^2) \\ &= 1 - q - q\sum_{x\in\mathbb{F}_q^*}\chi((a^q+a)^{-2}b^{q+1}x^{e_2-2e_1})\ , \qquad (3) \end{aligned}$$

and because $\gcd(q-1, 2e_1 - e_2) = 1$, we conclude that $T_{(e_1,e_2)}(a,b) = 1$.

For the case when q is odd, we first prove that $T_{(1,1)}(a,b) = 1$. Thus, by making the variable substitution $x \mapsto b^{-(q+1)}y^{-2}x$, in the inner summation of (2) (recall $e_1 = e_2 = 1$), we get

$$T_{(1,1)}(a,b) = -\sum_{z\in\mathbb{F}_q^*}\chi(z)\sum_{x\in\mathbb{F}_q^*}\chi(z^{-1}x)\sum_{y\in\mathbb{F}_q^*}\chi(b^{-(q+1)}(a^q+a)xy^{-1}) = 1\ .$$

Now suppose that q is odd and that e_1 and e_2 are any two integers. Then by Theorem 5.33 in R. Lidl and H. Niederreiter (1984) we know that, for all $\rho_0, \rho_1, \rho_2 \in \mathbb{F}_q$ with $\rho_2 \neq 0$,

$$\sum_{y\in\mathbb{F}_q^*}\chi(\rho_0 + \rho_1 y + \rho_2 y^2) = \chi(\rho_0 - \rho_1^2(4\rho_2)^{-1})\eta(\rho_2)G_{\mathbb{F}_q}(\eta,\chi) - \chi(\rho_0)\ ,$$

where η is the quadratic character of $\mathbb{F}_q$. Therefore, from (2), we have

$$T_{(e_1,e_2)}(a,b) = -\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\chi(z - cx^{2e_1-e_2}z)\eta(z^{-1}N_b x^{e_2})G_{\mathbb{F}_q}(\eta,\chi) - \chi(z)\ , \quad (4)$$

where $T_a := a^q + a$, $N_b := b^{q+1}$ and $c := 4^{-1}T_a^2 N_b^{-1}$. But q is odd and $\gcd(q+1, e_2) = 1$, therefore both e_2 and $2e_1 - e_2$ must be odd integers. Consequently, since $\gcd(q-1, 2e_1 - e_2) = 1$, there must exist an odd integer r such that $(2e_1 - e_2)r \equiv 1 \pmod{q-1}$. Therefore, by applying the variable substitution $x \mapsto x^r$ in the previous equality, we now have

$$T_{(e_1,e_2)}(a,b) = -\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\chi(z - cxz)\eta(z^{-1}N_b x^{re_2})G_{\mathbb{F}_q}(\eta,\chi) - \chi(z) ,$$

and since e_2 and r are both odd integers, clearly $\eta(z^{-1}N_b x^{re_2}) = \eta(z^{-1}N_b x)$. Therefore

$$\begin{aligned} T_{(e_1,e_2)}(a,b) &= -\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\chi(z - cxz)\eta(z^{-1}N_b x)G_{\mathbb{F}_q}(\eta,\chi) - \chi(z) \\ &= T_{(1,1)}(a,b) = 1 . \end{aligned}$$

For the proof of the converse, suppose that $\gcd(q-1, 2e_1 - e_2) = d > 1$. Thus, again by first supposing that q is even, we have from (3) that

$$\begin{aligned} T_{(e_1,e_2)}(a,b) &= 1 - q - qd\sum_{x\in\langle\delta^d\rangle}\chi((a^q + a)^{-2}b^{q+1}x) \\ &= 1 - q - qdt , \end{aligned}$$

for some integer t (recall that $\chi(w) = \pm 1$, for all $w \in \mathbb{F}_q$), and since $d > 1$, we have that $dt \neq -1$. Therefore $T_{(e_1,e_2)}(a,b) \neq 1$.

Finally, suppose that $\gcd(q-1, 2e_1 - e_2) = d > 1$ and that q is odd. In this case note that e_2 and d are also odd integers. Thus, since $\eta(x^{e_2}) = \eta(x^{2e_1 - e_2})$ for all $x \in \mathbb{F}_q^*$, we have from (4):

$$\begin{aligned} T_{(e_1,e_2)}(a,b) = & -\sum_{x\in\mathbb{F}_q^*}\sum_{z\in\mathbb{F}_q^*}\chi(z - cx^{2e_1-e_2}z)\eta(z^{-1}N_b x^{2e_1-e_2})G_{\mathbb{F}_q}(\eta,\chi) - \chi(z) \\ & = 1 - q - G_{\mathbb{F}_q}(\eta,\chi)\sum_{x\in\mathbb{F}_q^*}\eta(N_b x)\sum_{z\in\mathbb{F}_q^*}\chi((1 - cx^d)z)\eta(z^{-1}) , \end{aligned}$$

because $\gcd(q-1, 2e_1 - e_2) = d$ and $\eta(x^d) = \eta(x)$.

Now, if $\mathcal{B} := \{x \in \mathbb{F}_q^* \mid x^d = c^{-1}\}$, then observe that $|\mathcal{B}| = 0$ or $|\mathcal{B}| = d$, and

$$\sum_{x\in\mathcal{B}} \sum_{z\in\mathbb{F}_q^*} \chi((1-cx^d)z)\eta(z^{-1}) = \sum_{x\in\mathcal{B}} \sum_{z\in\mathbb{F}_q^*} \eta(z^{-1}) = 0 \ .$$

Therefore

$$\begin{aligned} T_{(e_1,e_2)}(a,b) &= 1-q-G_{\mathbb{F}_q}(\eta,\chi) \sum_{x\in\mathbb{F}_q^*\backslash\mathcal{B}} \eta(N_b x) \sum_{z\in\mathbb{F}_q^*} \bar{\chi}((cx^d-1)z)\bar{\eta}(z) \\ &= 1-q-G_{\mathbb{F}_q}(\eta,\chi) \sum_{x\in\mathbb{F}_q^*\backslash\mathcal{B}} \eta(N_b x) G_{\mathbb{F}_q}(\bar{\eta},\bar{\chi})\eta(cx^d-1) \ , \end{aligned}$$

where the last equality arises due to the Part (i) of Theorem 5.12 (p. 193) in R. Lidl and H. Niederreiter (1984). But $G_{\mathbb{F}_q}(\eta,\chi)G_{\mathbb{F}_q}(\bar{\eta},\bar{\chi}) = q$, therefore

$$\begin{aligned} T_{(e_1,e_2)}(a,b) &= 1-q-q \sum_{x\in\mathbb{F}_q^*\backslash\mathcal{B}} \eta(N_b x)\eta(cx^d-1) \\ &= 1-q-q \sum_{x\in\mathbb{F}_q^*\backslash\mathcal{B}} \eta(x)\eta(x^d-c^{-1}) \ , \end{aligned}$$

because $\eta(N_b) = \eta(c^{-1})$. Now, if $\mathcal{D} := \{\delta^i \mid 0 \le i < \frac{q-1}{d}\}$, then note that

$$|\mathcal{D}\cap\mathcal{B}| = \begin{cases} 0 & \text{if } |\mathcal{B}| = 0, \\ 1 & \text{if } |\mathcal{B}| = d. \end{cases}$$

Thus,

$$T_{(e_1,e_2)}(a,b) = 1-q-q \sum_{x\in\mathcal{D}\backslash(\mathcal{D}\cap\mathcal{B})} \sum_{j=0}^{d-1} \eta(x\delta^{j\frac{q-1}{d}})\eta((x\delta^{j\frac{q-1}{d}})^d - c^{-1}) \ ,$$

but since $\frac{q-1}{d}$ is even, we have $\eta(x\delta^{j\frac{q-1}{d}}) = \eta(x)$ and clearly $(x\delta^{j\frac{q-1}{d}})^d = x^d$. Therefore

$$\begin{aligned} T_{(e_1,e_2)}(a,b) &= 1-q-q \sum_{x\in\mathcal{D}\backslash(\mathcal{D}\cap\mathcal{B})} \sum_{j=0}^{d-1} \eta(x)\eta(x^d-c^{-1}) \\ &= 1-q-qd \sum_{x\in\mathcal{D}\backslash(\mathcal{D}\cap\mathcal{B})} \eta(x)\eta(x^d-c^{-1}) \\ &= 1-q-qdt \ , \end{aligned}$$

for some integer t (recall that $\eta(w) = \pm 1$, for all $w \in \mathbb{F}_q^*$), and since $d > 1$, we have that $dt \neq -1$. Therefore $T_{(e_1,e_2)}(a,b) \neq 1$. $\square$

Remark 2. *Let $\mathbb{F}_q$ be any finite field of odd characteristic and let η be the quadratic character of $\mathbb{F}_q$. If ρ is any nonzero element of $\mathbb{F}_q$ then note that, as a consequence of the previous proof, it is possible to conclude that*

$$|\{x \in \mathbb{F}_q^* \setminus \{\rho\} \mid \eta(x^2 - \rho x) = 1\}| = \frac{q-1}{2} - 1 \ .$$

We end this section of preliminary results by presenting the following

Corollary 1. *With the same notation as in the previous lemma, let $a, b \in \mathbb{F}_{q^2}$. If $\gcd(q-1, 2e_1 - e_2) = 1$ and $\gcd(q+1, e_2) = 1$, then*

$$T_{(e_1,e_2)}(a,b) = \begin{cases} (q-1)(q^2-1) & \textit{if} \quad a = 0 \textit{ and } b = 0, \\ -(q^2-1) & \textit{if } a^q + a \neq 0 \textit{ and } b = 0, \\ -(q-1) & \textit{if } a^q + a = 0 \textit{ and } b \neq 0, \\ 1 & \textit{if } a^q + a \neq 0 \textit{ and } b \neq 0. \end{cases}$$

Proof: Clearly $T_{(e_1,e_2)}(0,0) = (q-1)(q^2-1)$ and, if $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a) \neq 0$ and $b = 0$, then

$$\begin{aligned} T_{(e_1,e_2)}(a,0) &= \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^2}^*} \chi'(a x^{(q+1)e_1} y) \\ &= \sum_{x \in \mathbb{F}_{q^2}^*} \sum_{y \in \mathbb{F}_q^*} \chi(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a) x^{(q+1)e_1} y) = -(q^2-1) \ . \end{aligned}$$

On the other hand, if $a^q + a = 0$ and $b \neq 0$, then

$$\begin{aligned} T_{(e_1,e_2)}(a,b) &= \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^2}^*} \chi(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a) x^{(q+1)e_1} y) \chi'(b x^{e_2} y) \\ &= \sum_{x \in \mathbb{F}_{q^2}^*} \sum_{y \in \mathbb{F}_q^*} \chi(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(b x^{e_2}) y) \\ &= \sum_{i=0}^{q} \sum_{x \in \mathbb{F}_q^*} \sum_{y \in \mathbb{F}_q^*} \chi(x^{e_2} \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(b \gamma^{i e_2}) y) \ , \end{aligned}$$

but, since $\gcd(q+1,e_2)=1$, we have

$$\begin{aligned} T_{(e_1,e_2)}(a,b) &= \sum_{i=0}^{q}\sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\chi(x^{e_2}\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(b\gamma^i)y) \\ &= \sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\chi(0)+q\sum_{x\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\chi(y) \\ &= (q-1)^2-q(q-1)=-(q-1)\ . \end{aligned}$$

Finally, the proof of the last case comes from previous lemma. □

5. Formal proof of Theorem 1

We are now able to present a formal proof of Theorem 1.

Proof: Part (A): Clearly $(q+1)e_1q \equiv (q+1)e_1 \pmod{q^2-1}$ and, due to the fact that $\gcd(q+1,e_2)=1$, we have $e_2q \not\equiv e_2 \pmod{q^2-1}$, therefore $\deg(h_{(q+1)e_1}(x))=1$ and $\deg(h_{e_2}(x))=2$. Note that if $\mathcal{C}_{((q+1)e_1)}$ and $\mathcal{C}'_{((q+1)e_1)}$ are the cyclic codes with the same parity-check polynomial $h_{(q+1)e_1}(x)$, and whose lengths are, respectively, q^2-1 and $q-1$, then the weights of all codewords of these two codes differ just by the constant factor $q+1$. Now by using the set of characterizations, for the one-weight irreducible cyclic codes, that was introduced in Theorem 11 of G. Vega (2007), and since $\gcd(\frac{q^1-1}{q-1},(q+1)e_1)=1$, we conclude that $\mathcal{C}'_{((q+1)e_1)}$ is a cyclic code of length $q-1$, whose nonzero weight is $q-1$. Therefore the nonzero weight of $\mathcal{C}_{((q+1)e_1)}$ is q^2-1. On the other hand, because $\gcd(\frac{q^2-1}{q-1},e_2)=1$, we can conclude, in a similar manner, that $h_{e_2}(x)$ is the parity-check polynomial of a one-weight cyclic code of length q^2-1, whose nonzero weight is $q(q-1)$.

Part (B): Clearly, the cyclic code $\mathcal{C}_{((q+1)e_1,e_2)}$ has length q^2-1 and its dimension is 3 due to Part (A). Let $\mathcal{A}$ be a fixed subset of $\mathbb{F}_{q^2}^*$ in such a way that $|\mathcal{A}|=q-1$ and $\{\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a)\mid a\in\mathcal{A}\}=\mathbb{F}_q^*$ (observe that if q is even, then the subset $\mathcal{A}$ must be different from $\mathbb{F}_q^*$). Now, for each $a\in\mathcal{A}\cup\{0\}$ and $b\in\mathbb{F}_{q^2}$, we define $c(q^2-1,e_1,e_2,a,b)$ as the vector of length q^2-1 over $\mathbb{F}_q$, which is given by:

$$(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a(\gamma^{(q+1)e_1})^i+b(\gamma^{e_2})^i))_{i=0}^{q^2-2}\ .$$

Thanks to Delsarte's Theorem (P. Delsarte (1975)) it is well known that

$$\mathcal{C}_{((q+1)e_1,e_2)} = \{c(q^2-1,e_1,e_2,a,b) \mid a \in \mathcal{A} \cup \{0\} \text{ and } b \in \mathbb{F}_{q^2}\} \ .$$

Thus the Hamming weight of any codeword $c(q^2-1,e_1,e_2,a,b)$, in our cyclic code $\mathcal{C}_{((q+1)e_1,e_2)}$, will be equal to $q^2-1-Z(a,b)$, where

$$Z(a,b) = \sharp\{\ i \mid \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a\gamma^{(q+1)e_1 i} + b\gamma^{e_2 i}) = 0,\ 0 \le i < q^2-1\} \ .$$

If χ' and χ are, respectively, the canonical additive characters of $\mathbb{F}_{q^2}$ and $\mathbb{F}_q$, then

$$\begin{aligned} Z(a,b) &= \frac{1}{q}\sum_{i=0}^{q^2-2}\sum_{y\in\mathbb{F}_q}\chi(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(y(a\gamma^{(q+1)e_1 i} + b\gamma^{e_2 i}))) \\ &= \frac{q^2-1}{q} + \frac{1}{q}\sum_{y\in\mathbb{F}_q^*}\sum_{x\in\mathbb{F}_{q^2}^*}\chi'(yax^{(q+1)e_1} + ybx^{e_2}) \ , \end{aligned}$$

and, by using the notation of Lemma 3, we have

$$Z(a,b) = \frac{q^2-1}{q} + \frac{1}{q}T_{(e_1,e_2)}(a,b) \ . \tag{5}$$

But $\gcd(q-1,2e_1-e_2)=1$ and $\gcd(q+1,e_2)=1$; therefore, after applying Corollary 1, we get

$$Z(a,b) = \begin{cases} q^2-1 & \text{if } a=0 \text{ and } b=0, \\ 0 & \text{if } a\in\mathcal{A} \text{ and } b=0, \\ q-1 & \text{if } a=0 \text{ and } b\neq 0, \\ q & \text{if } a\in\mathcal{A} \text{ and } b\neq 0. \end{cases}$$

Consequently, the assertion about the weight distribution of $\mathcal{C}_{((q+1)e_1,e_2)}$ comes now from the fact that the Hamming weight of any codeword in $\mathcal{C}_{((q+1)e_1,e_2)}$ is equal to $q^2-1-Z(a,b)$, and also due to the fact that $|\mathcal{A}| = q-1$ and $|\mathbb{F}_{q^2}^*| = q^2-1$.

Lastly, $\mathcal{C}_{((q+1)e_1,e_2)}$ is an optimal cyclic code, due to Lemma 1, and the assertion about the weights of the dual code $\mathcal{C}_{((q+1)e_1,e_2)}$ can now be proved by means of Table I and the first four identities of Pless (see, for example, pp. 259-260 in W.C. Huffman and V.S. Pless (2003)). □

Due to the simplicity of the numerical conditions in Theorem 1, it is possible to compute the total number of different cyclic codes, over $\mathbb{F}_q$, of length q^2-1 and dimension 3, that satisfy such conditions. The following result goes in that direction.

Theorem 4. *With our notation, let $\mathcal{N}$ be the number of different cyclic codes, $\mathcal{C}_{((q+1)e_1,e_2)}$, of length q^2-1 and dimension 3 that satisfy conditions in Theorem 1. Then*

$$\mathcal{N} = \frac{\phi(q^2-1)(q-1)}{2}\,, \tag{6}$$

where ϕ denotes the Euler ϕ-function.

Proof: Since $\deg(h_{e_2}(x)) = 2$, the total number, $\mathcal{N}_2$, of different minimal polynomials $h_{e_2}(x)$ that satisfy condition $\gcd(q+1,e_2)=1$ is $\mathcal{N}_2 = \frac{\phi(q+1)(q-1)}{2}$. On the other hand, since $\deg(h_{(q+1)e_1}(x)) = 1$ we have that, for each integer e_2 that satisfies $\gcd(q+1,e_2)=1$, the total number, $\mathcal{N}_1$, of different minimal polynomials $h_{(q+1)e_1}(x)$ that satisfy condition $\gcd(q-1,2e_1-e_2)=1$ is

$$\begin{aligned}\mathcal{N}_1 &= |\{0 \leq e_1 < (q-1) \mid \gcd(q-1,2e_1-e_2)=1\}|\\ &= \begin{cases} \phi(q-1) & \text{if } q \text{ is even,}\\ 2\phi(q-1) & \text{otherwise.}\end{cases}\end{aligned}$$

But since $\mathcal{N} = \mathcal{N}_1\mathcal{N}_2$, the result now follows from the fact that

$$\phi(q+1)\phi(q-1) = \begin{cases} \phi(q^2-1) & \text{if } q \text{ is even,}\\ \phi(q^2-1)/2 & \text{otherwise.}\end{cases}$$

□

The following are examples related to Theorem 1 and Theorem 4.

Example 1. *With the same notation as in Theorem 1, let $q=4$, $e_1=2$ and $e_2=6$. Then $\gcd(q-1,2e_1-e_2)=1$ and $\gcd(q+1,e_2)=1$. Therefore, by Theorem 1, we can be sure that $\mathcal{C}_{(10,6)}$ is an optimal three-weight cyclic code over $\mathbb{F}_4$, of length 15, dimension 3 and weight enumerator polynomial*

$$1+45z^{11}+15z^{12}+3z^{15}\,. \tag{7}$$

In addition, $B_1=B_2=0$ and $B_3=195$. In fact, the dual code of $\mathcal{C}_{(10,6)}$ is a $[15,12,3]$ cyclic code which, by the way, has the same parameters as the best known linear code, according to the tables of the best known linear codes maintained by Markus Grassl at http://www.codetables.de/.

Example 2. *Again, we take $q = 4$. Then, owing to Theorem 4, the total number of different cyclic codes, over $\mathbb{F}_4$, of length 15 and dimension 3 that satisfy conditions of Theorem 1 is $\mathcal{N} = 12$. In fact, these cyclic codes are $\mathcal{C}_{(0,1)}$, $\mathcal{C}_{(0,2)}$, $\mathcal{C}_{(0,7)}$, $\mathcal{C}_{(0,11)}$, $\mathcal{C}_{(5,1)}$, $\mathcal{C}_{(5,3)}$, $\mathcal{C}_{(5,6)}$, $\mathcal{C}_{(5,7)}$, $\mathcal{C}_{(10,2)}$, $\mathcal{C}_{(10,3)}$, $\mathcal{C}_{(10,6)}$ and $\mathcal{C}_{(10,11)}$. Now, through a direct inspection it is interesting to note that all different cyclic codes over $\mathbb{F}_4$ of length 15, dimension 3 and weight enumerator polynomial as in (7), are exactly those listed before.*

6. Towards the characterization

Through the last example in the previous section, it can be conjectured that the sufficient numerical conditions in Theorem 1 are also the necessary conditions. In fact, this is the real situation and the following result gives us a formal proof of this conjecture.

Theorem 5. *Let $\mathcal{C}$ be a cyclic code of length $q^2 - 1$ over a finite field $\mathbb{F}_q$. Then, the weight distribution of $\mathcal{C}$ is given in Table I if and only if its dimension is 3 and there exist two integers, e_1 and e_2, in such a way that $h_{(q+1)e_1}(x)h_{e_2}(x)$ is the parity-check polynomial of $\mathcal{C}$, and the two integers satisfy* $\gcd(q-1, 2e_1 - e_2) = 1$ *and* $\gcd(q+1, e_2) = 1$.

Proof: Suppose that $\mathcal{C}$ is a cyclic code of length $q^2 - 1$ over a finite field $\mathbb{F}_q$, whose weight distribution is given in Table I. Through the sum of the frequencies of such table, it is easy to see that $\mathcal{C}$ must be a cyclic code of dimension 3. Consequently, the degree of the parity-check polynomial $h(x)$, of $\mathcal{C}$, must be equal to 3. Since $(q^2 - 1) \nmid (q^3 - 1)$, the code $\mathcal{C}$ cannot be an irreducible cyclic code of length $q^2 - 1$ and dimension 3. Therefore the parity-check polynomial $h(x)$ must be reducible. As was explained in the proof of Part (A) of Theorem 1, a cyclic code of length $q^2 - 1$ and dimension 1 is just a one-weight irreducible cyclic code over $\mathbb{F}_q$, whose nonzero weight is $q^2 - 1$. Thus, if $h(x)$ is the product of three polynomials of degree 1, then $\mathcal{C}$ will correspond to the span of the union of three different one-weight irreducible cyclic codes (seeing them as three different subspaces of $\mathbb{F}_q^{q^2-1}$), and therefore the frequency of the nonzero weight of $q^2 - 1$, in Table I, should be at least $3(q-1)$. Since this is not the situation for Table I, the polynomial $h(x)$ must be the product of two polynomials, one of them of degree 1 and the other one of degree 2. Seeing such polynomials as minimal polynomials over $\mathbb{F}_{q^2}$, we have that there must exist two integers e_1 and e_2 in such a way that $h(x) = h_{(q+1)e_1}(x)h_{e_2}(x)$.

Now, we are going to prove that $\gcd(q+1, e_2) = 1$. Let $\mathcal{C}_{((q+1)e_1)}$ and $\mathcal{C}_{(e_2)}$ be the cyclic codes of length q^2-1 over $\mathbb{F}_q$, whose parity-check polynomials are, respectively, $h_{(q+1)e_1}(x)$ and $h_{e_2}(x)$. If $\gcd(q+1, e_2) = u > 1$, then, due to the set characterizations for the one-weight irreducible cyclic codes, that was introduced in G. Vega (2007), $\mathcal{C}_{(e_2)}$ must have at least two nonzero weights. Since $\mathcal{C}_{((q+1)e_1)}$ is a one-weight irreducible cyclic code of length q^2-1, with nonzero weight q^2-1, and due to the fact that $\mathcal{C}$ is the span of the union of $\mathcal{C}_{((q+1)e_1)}$ and $\mathcal{C}_{(e_2)}$, we have that none of the nonzero weights of $\mathcal{C}_{(e_2)}$ can be equal to q^2-1. But in Table I there are just 3 different nonzero weights and one of them is equal to q^2-1. Thus the conclusion here is that if $\gcd(q+1, e_2) = u > 1$, then $\mathcal{C}_{(e_2)}$ will correspond to a two-weight irreducible cyclic code, over $\mathbb{F}_q$, of length q^2-1 and dimension 2, whose nonzero weights are $q(q-1)$ and $q(q-1)-1$. Fortunately for us, simple necessary and sufficient numerical conditions for an irreducible cyclic code to have at most two weights were presented in the remarkable work of B. Schmidt and C. White (2002). Despite the fact that such characterization is just for all two-weight irreducible cyclic codes over a prime field, the authors provided all the required clues to extend their characterization to *any* finite field. Thus, taking into consideration these clues it is possible to obtain the following characterization for all the two-weight irreducible cyclic codes of length q^2-1 and dimension 2 over any finite field (see Theorem 6 and its proof in G. Vega (2015)).

TABLE II

Weight distribution of a two-weight code $\mathcal{C}_{(e)}$.

Here $\varepsilon = \pm 1$ is determined by $rp^{s\theta} \equiv \varepsilon \pmod{u}$.

Weight	**Frequency**
0	1
$\frac{q-1}{q}(q^2 - r\varepsilon p^{s\theta})$	$\frac{(q^2-1)(u-r)}{u}$
$\frac{q-1}{q}(q^2 + (u-r)\varepsilon p^{s\theta})$	$\frac{(q^2-1)r}{u}$

Theorem 6. *Let p, t and q be positive integers in such a way that p is a prime number and $q = p^t$. For any integer e, let $\mathcal{C}_{(e)}$ be the irreducible cyclic code, over $\mathbb{F}_q$, of length q^2-1, whose parity-check polynomial is $h_e(x)$, and suppose that* $\deg(h_e(x)) = 2$. *For $u = \gcd(q+1, e)$, let f and s be the two integers in such a way that $2t = fs$, with $f := ord_u(p)$ (that is, f is*

the multiplicative order of p modulo u). *For a positive integer x, let $S_p(x)$ denote the sum of the p-digits of x. Define*

$$\theta(u,p) = \frac{1}{p-1} \min \left\{ S_p\left(\frac{j(p^f-1)}{u} \right) \mid 1 \leq j < u \right\} ,$$

and fix $\theta = \theta(u,p)$. Then the irreducible cyclic code $\mathcal{C}_{(e)}$ has the weight distribution given in Table II if and only if $u > 1$ and there exists a positive integer r satisfying

$$\begin{aligned} & r|(u-1) \\ & rp^{s\theta} \equiv \pm 1 \pmod{u} \\ & r(u-r) = (u-1)p^{s(f-2\theta)} \ . \end{aligned}$$

Now, by observing Table II and by noting that r and $u-r$ cannot be zero in the previous theorem, we have that the nonzero weights of any two-weight irreducible cyclic code of length q^2-1 and dimension 2 can never be equal to $q(q-1)$. But this is a contradiction, because we already conclude that the nonzero weights of $\mathcal{C}_{(e_2)}$ are $q(q-1)$ and $q(q-1)-1$. Therefore $\mathcal{C}_{(e_2)}$ cannot be a two-weight irreducible cyclic code, and in consequence, $\gcd(q+1, e_2) = 1$.

It remains to prove that $\gcd(q-1, 2e_1-e_2) = 1$. If $\gcd(q+1, e_2) = 1$, then, once again, as was explained in proof of Part (A) of Theorem 1, $\mathcal{C}_{(e_2)}$ will correspond to a one-weight irreducible cyclic code of length q^2-1 and dimension 2, whose nonzero weight is $q(q-1)$. Since the frequency of such nonzero weight is $q^2-1 = |\mathbb{F}_{q^2}^*|$, in Table I, we have that a codeword, c, in $\mathcal{C}$ will have Hamming weight $q(q-1)-1$ if and only if $c = c_1 + c_2$, where c_1 and c_2 are, respectively, two nonzero codewords in $\mathcal{C}_{((q+1)e_1)}$ and $\mathcal{C}_{(e_2)}$. But if c_1 and c_2 are nonzero codewords in $\mathcal{C}_{((q+1)e_1)}$ and $\mathcal{C}_{(e_2)}$, then there must exist two finite field elements a and b in $\mathbb{F}_{q^2}$, with $a^q + a \neq 0$, $b \neq 0$, in such a way that the number of zero entries, $Z(a,b)$, in codeword c, can be computed by means of (5). Under these circumstances, codeword c will have Hamming weight $q(q-1)-1$ if and only if $T_{(e_1,e_2)}(a,b) = 1$, and due to Lemma 3, this can only be possible if and only if $\gcd(q-1, 2e_1-e_2) = 1$.

Finally, the proof of the converse is just a part of the proof of Theorem 1 that was already given in previous section. □

As a direct consequence of Theorems 4 and 5, we have the following result.

Corollary 2. *Let $\mathcal{N}$ be the number of different cyclic codes of length $q^2 - 1$, over $\mathbb{F}_q$, whose weight distribution is given in Table I. Then $\mathcal{N}$ is given by (6).*

7. Conclusions

In this work we presented a characterization of a class of optimal three-weight cyclic codes of length $q^2 - 1$ and dimension 3, over any finite field $\mathbb{F}_q$. The codes under this characterization are, indeed, optimal in the sense that their lengths reach the Griesmer lower bound for linear codes. In addition, we also found the parameters for the dual code of any cyclic code in this class. In fact, throughout several studied examples, it seems that such dual codes have always the same parameters as the best known linear codes. As we saw in Example 2, it is easy to find all cyclic codes over a fixed finite field $\mathbb{F}_q$ of length $q^2 - 1$ and dimension 3 that satisfy the two conditions of Theorem 1. But due to Theorem 5 we can be sure that these cyclic codes will be all optimal three-weight cyclic codes of length $q^2 - 1$, whose weight distribution is given in Table I. As a complement of this work, we believe that it could be interesting the study of the family cyclic codes of length $q^2 - 1$, whose parity-check polynomial is in the form of $h(x) = h_{(q+1)e_1}(x)h_{e_2}(x)$, where the integers e_1 and e_2 satisfy $\gcd(q - 1, 2e_1 - e_2) > 1$ and $\gcd(q + 1, e_2) = 1$.

References

P. Delsarte, On subfield subcodes of Reed-Solomon codes, IEEE Trans. Inf. Theory, IT-21(5) (1975) 575-576.

C. Ding, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inf. Theory 55(3) (2009) 955-960.

T. Feng, A Characterization of Two-Weight Projective Cyclic Codes, IEEE Trans. Inf. Theory 61(1) (2015) 66-71.

J.H. Griesmer, A bound for error correcting codes, IBM J. Res. Dev. 4 (1960) 532-542.

W.C. Huffman and V.S Pless, Fundamental of Error-Correcting Codes. Cambridge Univ. Press, Cambridge, 2003.

C. Li, N. Li, T. Helleseth and C. Ding, The weight distribution of several classes of cyclic codes from APN monomials, IEEE Trans. Inf. Theory 60 (2014) 4710-4721.

C. Li, Q. Yue and F. Li, Weight distributions of cyclic codes with respect to pairwise coprime order elements, Finite Fields Appl. 28 (2014) 94-114.

R. Lidl and H. Niederreiter H, Finite Fields. Cambridge Univ. Press, Cambridge, 1984.

M.J. Moisio, On relations between certain exponential sums and multiple Kloosterman sums and some applications to coding theory, preprint (1997) 1-11.

B. Schmidt and C. White, All two-weight irreducible cyclic codes?, Finite Fields and their Appl. 8 (2002) 1-17.

G. Solomon and J.J. Stiffler, Algebraically punctured cyclic codes, Inform. and Control 8 (1965) 170-179.

G. Vega, Determining the number of one-weight cyclic codes when length and dimension are given. Lecture Notes in Comput. Sci. 4547 (2007) 284-293.

G. Vega, Two-weight cyclic codes constructed as the direct sum of two one-weight cyclic codes, Finite Fields Appl. 14(3) (2008) 785-797.

G. Vega, A critical review and some remarks about one- and two-weight irreducible cyclic codes, Finite Fields Appl. 33 (2015) 1-13.

J. Yuan, C. Carlet and C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory 52(2) (2006) 712-717.

Z. Zhou and C. Ding, A class of three-weight cyclic codes, Finite Fields Appl. 25 (2013) 79-93.